**3GPP TSG-SA3 Meeting #107-e *S3-221091***

**e-meeting, 16 – 20 May 2022 Revision of S3-22xxxx**

|  |
| --- |
| *CR-Form-v12.1* |
| **DRAFT CHANGE REQUEST** |
|  |
|  | **33.926** | **CR** | **Draft-CR** | **rev** | **-** | **Current version:** | **17.3.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Threat modifications for token verification |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G\_Ph2 |  | ***Date:*** |  2022-05-16 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-18 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | According to TS 33.501, for SNPNs with Credentials Holder using AUSF and UDM for primary authentication, similar authorization mechanisms with roaming are adopted to ensure the service authorization between SNPN and credentials holder. If token verification does not include the SNPN ID in the same way with PLMN ID in roaming, the service will be consumed by unauthorized SNPN.According to TS 33.501, for SNPNs with Credentials Holder using AUSF and UDM for primary authentication, similar authorization mechanisms with roaming are adopted to ensure the service authorization between SNPN and credentials holder. If SEPP does not check the SNPN ID in the same way with PLMN ID in roaming, the service will be consumed by unauthorized SNPN. |
|  |  |
| ***Summary of change:*** | Modify the token verification threat to also cover the SNPN case.Modify the PLMN ID mismatch threat to also cover the SNPN case |
|  |  |
| ***Consequences if not approved:*** | The threat evaluation for SNPN is missed.The threat evaluation for SNPN is missed. |
|  |  |
| ***Clauses affected:*** | 6.3.3.1，G.2.3.1 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **x** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **x** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **x** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*.

### 6.3.3 Threats related to service access

#### 6.3.3.1 Elevation of privilege via incorrect verification of access tokens

- *Threat name*: Incorrect Verification of Access Tokens.

- *Threat category*: Elevation of Privilege, Information Disclosure, Denial of Service.

- *Threat Description*: there are following threats if the generic NF cannot correctly verify the access tokens:

- An access token may be tampered so that an attacker can arbitrarily access any services from any NF service providers within the same PLMN or in different PLMNs or SNPNs, which leads to elevation of privilege and consequently information disclosure.

- An access token may be tampered so that an attacker can arbitrarily access the services of any slices provided by the NF producer instances (excluded from the list of NSSAIs or the list NSI IDs) within the same PLMN or in different PLMNs or SNPNs, which leads to elevation of privilege and consequently information disclosure.

- An access token may be tampered so that an attacker can arbitrarily access the services provided by the NF producer instances outside the NF Set which it is allowed to access within the same PLMN or in different PLMNs or SNPNs, which leads to elevation of privilege and consequently information disclosure.

- An access token may be tampered so that an attacker can arbitrarily access the disallowed resources or conduct disallowed actions on the resources for the services provided by a NF service provider within the same PLMN or in different PLMNs or SNPNs, which leads to elevation of privilege and consequently information disclosure.

- An access token may be tampered so that an attacker can block service access by replacing the granted services/NF service providers with unavailable services/NF service providers, which leads to denial of service.

- An expired access token can be replayed so that an attack can access the services which may no longer be allowed by the NF service provider, which leads to elevation of privilege and consequently information disclosure.

*- Threatened Asset:* NF API data, NF Application, Sufficient processing capacity

NOTE x: This SNPNs authorization aspects only apply to UDMs, NRFs and AUSFs in Credentials Holders Credentials Holder using AUSF and UDM for primary authentication.\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## G.2.3 Threats related to error handling in the SEPP

### G.2.3.1 Incorrect handling for PLMN ID or SNPN ID mismatch

*- Threat name:* Incorrect handling for PLMN ID or SNPN ID mismatch

*- Threat Category*: Denial of Service, Information Disclosure, Spoofing Identity

*- Threat Description*: there are following threats if the SEPP does not make correct handling when detecting that the PLMN-ID or SNPN ID contained in the incoming N32-f message does not match the PLMN-ID or SNPN ID in the related N32-f context:

- Without receiving error signalling message from the SEPP which detected the mismatch, the peer SEPP is not aware of such error and will continue to send the messages with errors. This can result in waste of system resources.

- If the SEPP sends an error signalling message without indicating the error cause and the corresponding N32-f message ID, the peer SEPP is not able to identify what error occurs and what is the source message on which the error occurs. Hence the peer SEPP is not able to take actions accordingly. This can result in service interruption as well as waste of system resources.

- The serving PLMN ID or SNPN ID appended in the subject claim of the access token sent by a NF service consumer in the serving PLMN will not be checked by the NF service producer in the home PLMN. If the SEPP in the HPLMN detected the mismatch of serving PLMN ID or SNPN ID in the access token but still forwards the NF Service Request to the NF service producer, the serving PLMN ID or SNPN ID mismatch will not be detected by the NF service producer and the request will be wrongly accepted if all the other checks on the access token get passed. This can result in unauthorized service access by NF service consumer as well as waste of system resources.

*- Threatened Asset*: Application layer security data, Sufficient Processing Capacity

NOTE x: SNPN ID mismatch only applies to SEPPs in a Credentials Holder using AUSF and UDM for primary authentication.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*